



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/462,616	04/03/2000	GUNTER MARINGER	0745/61002/N	5313

7590 04/08/2004

NORMAN H ZIVIN
COOPER & DUNHAM
1185 AVENUE OF THE AMERICAS
NEW YORK, NY 10036

EXAMINER

KLIMACH, PAULA W

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 04/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/462,616

Applicant(s)

MARINGER ET AL.

Examiner

Paula W Klimach

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 09 January 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-14 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 1/9/04 (Paper No. 8). Original application contained Claims 1-14. Applicant amended Claims 1-14. The amendment filed on 1/9/04 have been entered and made of record. Therefore, presently pending claims are 1-14.

Response to Arguments

Applicant's arguments filed 1/9/04 have been fully considered but they are not persuasive because of following reasons given in the rejection below.

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that the prior art does teach or suggest the subject matter broadly recited in independent Claim 1. Dependent Claims 2-14 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action (Paper No. 7). Accordingly, rejections for claims 1-14 are respectfully maintained.

Claim Rejections - 35 USC § 112

Claim 1 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described

Art Unit: 2135

in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 1 discloses, "sending a second random number (Challenge 2)," from the terminal to the network.

Although the original specification the applicants disclose a Challenge 2 that is sent to the network, this challenge response system is a prior art system (Fig. 1, page 13 paragraph 1 and 2). In the new method (Fig. 2, paragraph 2 and 3), "it is sufficient for N to send only the data set Response 2 to M for authentication." Indeed, fig. 2 only shows the Challenge 1 being sent from the network to the terminal. The Challenge 2 is not sent, even though the Response 2 is sent from the terminal to the network. Further, in Fig. 3 page 14, the network sends the Challenge 1 and Response 2 in the first message and then the terminal sends the Response 1 in the next message. No Challenge 2 is sent.

To expedite a complete examination of the instant application the claims rejected under 35 U.S.C 112 above are further rejected as set forth below in assuming that the new matter has been removed, therefore the Challenge 2 is not sent to the network from the terminal.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over the article by Clark et al.

Clark discloses a method for mutual authentication of components in a network using a challenge-response method to authenticate a Principal A with the Principal B (section 6.3.1), comprising the steps of:

Requesting at least one data pair including a first random number (Challenge 1) and a first response (Response 1) from an authentication center using a request from the network. Clark discloses the Principal A requesting the data for authentication from the server S. The authentication data of the system disclosed by Clark is used like the data pair. The first challenge ($E(K_{bs}: Kab, A)$) and the first response is Kab.

Passing the first random number (Challenge 1) to the terminal which uses an internally stored key and the first random number to calculate the first response (Response 1). The Principal A sends the first challenge to the Principal B in the 3rd message ($E(K_{bs}: Kab, A)$). This challenge is a random number since keys are random numbers and the key, therefore the key Kab is a random number and encrypting a random number produces a random number, therefore the value ($E(K_{bs}: Kab, A)$) is a random number. The principal B has the internally stored key Kbs, which is used to decrypt Kab.

Sending the calculated first response to the network. The Principal B sends principal A the calculated first response in message number 4. The Principal B calculates the first response Kab by decrypting the challenge 1 and then sends principal A the value of Kab by encrypting the nonce Nb.

Responding to the second random number with a second response (Response 2). Where the Principal A sends the Principal B the second response $Nb-1$. The second response is sent to the Principal B by encrypting the nonce using the encryption key Kab .

The response performed by the network, wherein the first response (Response 1) sent from the terminal to the network is also used as the second random number (Challenge 2). Whereby the network has previously requested the second response (Response 2) from the authentication center together with the first random number and the first response as a triplet data set (Challenge 1/ Response 1/ Response 2). The second challenge is also used as the first response in that the first response to find the value of the key Kb the Principal B needs to know Kbs . Therefore the first response uses Kab to encrypt Nb and the first challenge is that if principal A has Kab then they should can decrypt Nb and calculate $Nb-1$. Therefore the first response uses Nb and Kb and the second challenge uses Nb and Kb . However the principal B does not have to send a challenge to principal A because they both know Kab and Nb .

Clarke does not expressly disclose the server S calculating the value of Nb , in the section 6.3.1 Needham Schroeder's Protocol with Conventional keys. However, Clarke does disclose in the section 6.3.4 Amended Needham Schroeder Protocol. The server S calculating Nb^0 form which Ba calculates Nb , therefore the server S calculates Nb indirectly (Section 6.3.4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to make the amendment to the Needham Schroeder system as disclosed in section 6.3.4. One of ordinary skill in the art would have been motivated to do this because this would create a fix for the Principal B not knowing the freshness of the key Kab sent by the principal A.

1. **Claims 2-14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Clarke as applied to claim 1 above, and further in view of Tsubakiyama (5,544,245).

In reference to claims 2 and 7, Clarke does not expressly disclose a method wherein the network interprets the calculated first response sent back from the terminal as the second random number.

Tsubakiyama suggests a method (Fig. 2) where the message sent from the network N (C1) is used as a challenge to the user named i who interprets the challenge and responds to the challenge with the response C2. Therefore, the challenge is a message, which is interpreted and a response to the challenge is created and sent.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the response given by the terminal in the system of Clark as the challenge as in the method of Tsubakiyama. One of ordinary skill in the art would have been motivated to do this because it would provide a mutual authentication which enables the network and each user to authenticate each other without inviting the chosen plaintext attack and the known plaintext attack on the encryption algorithm in the authentication protocol and permits the deliver of a key for cipher communication without the need of increasing the amount of data to be transmitted for the protocol for mutual authentication between the network and each user (Tsubakiyama column 2 lines 36-46).

In reference to claim 3, wherein the first random number (Challenge 1) and the second response (Response 2) are transmitted from the network (N) to the terminal (M) immediately successively in time. Section 6.3.7 in the system described by Clarke the challenge and response are relatively successively carried out.

In reference to claim 4, wherein the data pair (Challenge 1/Response 2) is transmitted from the network (N) to the terminal (M) simultaneously, in the form of a single data set.

Clark does not expressly disclose sending the Challenge 1 and Response 2 in one transmission over the network.

However, at the time the invention was made, it would have been obvious to a person of ordinary skill in the art to send the Challenge 1 and Response 2 in one transmission over the network if device has the technical capabilities. One of ordinary skill in the art would have been motivated to do this because consolidating the messages would reduce the traffic on the network.

In reference to claims 5 and 6, wherein the network requests data sets from the authentication center (AUC) in the form of triplet data sets (Challenge 1/Response 1/Response 2). Message 2 of section 6.3.1 discloses a system where the Challenge and response is sent to principal A.

In reference to claims 8-10, wherein the filling out process is carried out on a subscriber-specific basis, and wherein the complete length of the first response (Response 1) is shortened before transmission to the other station. Tsubakiyama discloses the manipulation of the data sent to the subscriber (user) to create a key (column 5 lines 12-15).

In reference to claim 11, wherein the network is a GSM network. Tsubakiyama discloses the network in Fig. 2. The GSM is a type of wireless network and therefore is encompassed in Tsubakiyama's description.

In reference to claim 12, wherein the network is a wire-based network. Tsubakiyama discloses a network in Fig. 2 which encompasses the wire-based network.

In reference to claim 13, wherein the individual, mutually authenticating components in a wire-based network are different monitoring units of computers which authenticate themselves with a central computer. Clark discloses a system with Principal A and Principal B that can be interpreted as any device on a network, which would encompass the description of monitoring units. The user in Tsubakiyama authenticates themselves to the network, which has a database of keys to use for communication with the different user. It therefore behaves like a central computer.

In reference to claim 14, wherein the AUC calculates the triplet data sets requested by the network and transmits these to the network off-line and independently of time, on request by the network, but in any case before the data interchange between the network and the terminal. Clark discloses the first and second messages (6.3.1) being used for receiving and requesting the authentication data. Therefore, this is performed before the communications between Principal A and Principal B.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

Art Unit: 2135

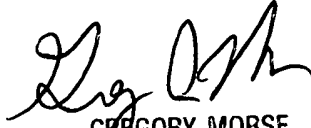
will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Monday, April 05, 2004


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100